Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2002

(U) This report was prepared by the Office of the National Counterintelligence Executive. Comments and queries are welcome and may be directed to the Chief, Analysis Group, NCIX, on (703) 874-8058.

Reverse Blank

NCIX 2003-10006
February 2003

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2002	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Annual Report to Congress on Foreign Economic Collection and Industrial Espionage: 2002	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the National Counterintelligence Executive (ONCIX) CS5 Room 300 Washington, DC 20505**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**20**	

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2002

Scope Note

This eighth annual report reviews the threat to the United States from foreign economic collection and industrial espionage. It seeks to assess efforts by foreign entities—government and private—to unlawfully target or acquire critical US technologies, trade secrets, and sensitive financial or proprietary economic information. The report focuses on technologies, the loss of which could undermine US military superiority, impede the ability of the United States to compete in the world marketplace, and/or have an adverse effect on the US economy, eventually weakening national security.

The report is being submitted in compliance with the Intelligence Authorization Act for Fiscal Year 1995, Section 809 (b), Public Law 103-359, which requires that the President annually submit to Congress updated information on the threat to US industry from foreign economic collection and industrial espionage. It updates the seventh *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, published in October 2001 and covers intelligence reporting and other information from calendar year 2001.

The National Counterintelligence Executive compiled this assessment using input from a broad cross section of US Government entities. The Department of Defense's Defense Security Service and the Air Force Office of Special Investigations collected significant amounts of data on illegal technology transfer and on economic and industrial espionage. Those data were instrumental in providing much of the detail for this assessment. The Federal Bureau of Investigation—the lead investigative agency for enforcing economic espionage statutes—also provided significant input. In addition, a host of other organizations made major contributions to and/or have coordinated on this report, including:

- Army Counterintelligence Center (ACIC).
- Central Intelligence Agency (CIA).
- Defense Intelligence Agency (DIA).
- Defense Threat Reduction Agency (DTRA).
- Department of Commerce (DOC).
- Department of Energy (DOE).

- Department of State, including the Bureau of Intelligence and Research (State/INR) and the Bureau of Diplomatic Security (State/DS).
- National Reconnaissance Office (NRO).
- National Security Agency (NSA).
- Naval Criminal Investigative Service (NCIS).

Contents

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2002

Key Findings

The United States was a prime target for foreign economic collection and industrial espionage and for the theft of export-controlled proprietary information in 2001, according to a variety of reporting. The openness of US society and the expanding international use of the Internet left the United States especially vulnerable. Foreign countries and companies used US technologies to leapfrog scientific hurdles that would otherwise have impeded their military and economic development. Calculating US losses from the technology outflow is difficult. Private estimates put the combined costs of foreign and domestic economic espionage, including the theft of intellectual property, as high as $300 billion per year and rising.

As in the past, militarily critical technologies (MCTs) were heavily targeted again in 2001. In fact, foreign collectors worked against all 18 MCTs, according to data provided to the Defense Security Service (DSS) by defense contractors. Almost one-third of suspicious incidents focused on information systems (IS), which have a wide range of military and civilian applications, while about a fifth went toward sensors and lasers—the eyes and ears of US military systems. Other MCTs that attracted significant attention included armaments and energetic materials, aeronautics, and electronics technology. Foreign collectors also actively pursued commercial trade secrets.

The efforts were not, as a rule, directed against the “crown jewels” of US technological supremacy. Instead, much of the sought after information and technology was dated military-related or infrastructure-supportive technologies that are no longer classified and that often have both military and civilian applications. Nor, in general, was this sensitive technology and information classified. It was, however, usually protected under US regulations.

The foreign sponsors of economic and industrial espionage in 2001 came from both the public and private sectors. The DSS database shows that the collection effort was spread almost evenly among the various actors—foreign government entities, government-affiliated agencies or foreign companies that work solely or predominantly for foreign governments, commercial businesses, and individuals whom DSS could not identify as affiliated with any of the above categories. Even where the suspicious inquiries originated from seemingly private firms, however, it is not possible to rule out some official sponsorship.

Some 75 countries—a mix of rich and poor, high- and low-tech, friend and foe—targeted US technologies in 2001 using a wide range of collection techniques. Simple, straightforward techniques, such as unsolicited requests for information or direct applications to purchase sensitive goods, were generally applied first and most frequently. When these proved ineffective, more sophisticated methods were used, such as offering to sell foreign goods and services as a means of gaining access to sensitive US facilities, targeting US experts abroad, or tasking foreign visitors to the United States with collection responsibilities. To a lesser extent, foreign collectors also attempted to exploit their existing relationships with US firms as a means to acquire sensitive equipment or technology and to employ the Internet and international conventions in their efforts.

There is every indication that efforts to acquire US economic and industrial secrets will only intensify and become more sophisticated over the next few years. US research and development programs ensure that state-of-the-art technology will continue to originate in the United States, and the openness of US society will make that technology a ready target to foreign countries and companies. The current top two or three players in this game are likely to remain major collectors for the foreseeable future. Other top spots, however, could change, depending on the state of global and regional tensions.

Foreign countries will continue to employ the whole gamut of collection tools in an effort to exploit available vulnerabilities. The easiest and cheapest methods will continue to be tried first. Although DSS reporting suggests that collectors in 2001 relied relatively less on the Internet as a tool than they have in the past, this is unlikely to be a harbinger of future trends. Collectors are likely to increasingly use Web sites to locate technology, e-mail to solicit technology, and cyber attacks to surreptitiously extract technology.

As to the types of militarily critical technologies that will be of interest over the next few years, IS probably will continue to top collectors' lists. In addition, aeronautics; guidance, navigation, and vehicle control systems; and sensors and lasers are certain to remain hot items. Space systems technologies, which in recent years have accounted for a relatively small share of suspicious incidents, may rate higher priorities in the future.

Annual Report to Congress on Foreign Economic Collection and Industrial Espionage—2002

The Threat to US National Security

The United States remains a prime target for economic espionage. Adversaries and allies alike continue to seek the United States' sophisticated technologies, manufacturing processes, information technology software and hardware, and financial information. Trade secrets and proprietary information of all types are fair game. The openness of US society and the expanding international use of the Internet have facilitated the incursions, making it easy and inexpensive for foreign businesspeople and government agents to acquire sensitive information and move it across national borders.

Private high-tech companies are particularly exposed to foreign exploitation because of this openness, but even secure US Government research organizations and laboratories that, at first glance, appear impervious to direct foreign access are being targeted. Most government organizations that deal with cutting-edge technologies, such as space systems and aeronautics, rely heavily on the facilities and expertise of outside contractors. Many of these contractors, in turn, work in industries that are engaged in the development of dual-use technologies and have contact with foreign collectors in the course of normal business. Foreign collectors—both private and government-sponsored—take full advantage of this indirect conduit into government operations.

For private foreign collectors, the prime motivation for stealing economic secrets is generally profits. Foreign companies may view the acquisition of trade secrets and proprietary information as the only way to compete against US companies that are moving up the technological ladder. Others see industrial espionage as key to gaining access to new markets dominated by more advanced US firms. Foreign individuals involved in the theft of state-of-the-art US technology may do so to bolster their stature in a foreign firm. Individual collectors also may be motivated by revenge. In a number of cases in 2001, individuals stole technology from US firms after they were notified that their employment had been terminated.

For foreign government collectors, the driving forces for industrial espionage against the United States can be more complex. The immediate goal of these efforts to acquire US technology probably is to leapfrog scientific hurdles without undertaking expensive and time-consuming research and development. For the larger and more advanced countries, the longer term objective appears to be to enable their military establishments to move closer to parity with the United States and to give their defense-industrial base and private companies a competitive edge in the global economy. Less developed countries, by contrast, often appear to tap the United States for defense capabilities that respond to known or perceived threats. Increasingly, the search for technology is also motivated by the knowledge that acquiring advanced weapons technology can significantly increase a small nation's power and influence. Collectors in underdeveloped countries are usually tasked with acquiring only small quantities of export-controlled goods, with the intent that domestic defense industries can cheaply reverse-engineer and mass-produce the products.

Putting an exact price tag on US losses stemming from the illegal outflow of trade secrets and proprietary information is difficult, but experts agree the costs are high and rising.[1] The American Society for Industrial Security (ASIS) estimated that US Fortune 1000 corporations may have lost more than $45 billion in 1999 from theft of their proprietary information and as much as $59 billion in 2001. ASIS estimated that losses from the theft of intellectual

[1] The estimated losses are associated with both foreign and domestic economic espionage.

The Data Problems

Populating databases with information that accurately reflects the level and variety of ongoing economic collection and industrial espionage is a difficult task.

- *Because the collection efforts are at best sensitive and at worst illegal, the CI community recognizes that some activity goes undetected and unreported.*
- *Even when US firms recognize that they have been subject to illegal espionage efforts, there are disincentives to reporting such incidents. Commercial firms are concerned how their stockholders or potential US Government customers might react to information that the company has been subject to even unsuccessful economic espionage attacks.*
- *It is not easy to determine whether a foreign inquiry for sensitive technology is part of a concerted effort to illegally acquire proprietary US information or simply an innocuous attempt by a foreign businessperson to obtain information that is thought to be unclassified and nonproprietary. Undoubtedly, some of the incidents that were reported as suspicious in 2001 by defense contractors were actually harmless attempts to legitimately acquire US products and technology.*
- *Given the dual-use nature of much of the sought after technology, it is often unclear even to the seller as to which goods and technologies are sensitive and, therefore, warrant reporting.*

The way the data is collected renders these databases of little use in trying to estimate changes in the level of economic espionage activity from one year to the next. The reporting relies on the responses of US companies. Those responses can fluctuate significantly from year to year even when the level of economic espionage goes unchanged. For example, periodic reminders by government officials to report activity can raise the profile of economic and industrial espionage efforts and lead to increased reporting. Also, major terrorist or CI events may increase threat awareness and spark additional reporting.

property for all US companies might be as high as $300 billion annually. As a broad indicator of the accelerating pace of global efforts to acquire US trade secrets, the annual survey conducted by the Computer Security Institute of San Francisco and the Federal Bureau of Investigation (FBI) showed 26 percent of companies reported intellectual property theft in 2001, up from 20 percent in 2000. Fewer than 1 percent of the firms surveyed were willing to attach figures to their losses of intellectual property, but the totals from those who made estimates amounted to $151 million in 2001, up from only about $67 million the previous year and $20 million in 1997.

The Most Sought After Information and Technologies

Foreign collectors targeted a broad range of technologies in 2001, including everything from sensitive militarily critical technologies (MCTs), which could be used to boost foreign defense capabilities, to more mundane business secrets that were apparently stolen for purely commercial reasons.

Militarily Critical Technologies—The Target of Choice

Indicating the broad scope of the 2001 collection effort, foreign collectors attempted to acquire all 18 of the technologies on the Department of Defense (DoD) Militarily Critical Technologies List (MCTL). Dual-use technologies—those that support military force modernization as well as enhance commercial ventures—were, again, the most sought after of the militarily critical items during the calendar year. The majority of defense technologies targeted were

components rather than complete systems, and this held particularly true for electronics. In addition, most of the targeted technology was unclassified, according to DSS data, although much of it was controlled under the International Traffic in Arms Regulations (ITAR) administered by the Department of State or the Export Administration Regulations (EAR) administered by the Department of Commerce.

Information systems (IS)—defined as the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information—topped the list of targeted MCTs, according to DSS data. In fact, 30 percent of all suspicious incidents reported in 2001 were

The 10 Most Highly Targeted US Militarily Critical Technologies, 2001

Militarily Critical Technology	Description	Number of Countries Targeting	Percent of Incidents[a]
Information Systems	The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.	40	30
Sensors and Lasers	Acoustic sensors for air, terrestrial, and marine platforms; sensors for locating submarines, mines, and lost objects; electro-optical sensors for night-vision devices and guidance for smart weapons; military lasers for limited visibility operations and to improve targeting accuracy with guided weapons.	38	20
Armaments and Energetic Materials	Technologies to develop and produce safe, affordable, storable, and effective conventional munitions and weapons systems of superior operational capability.	27	14
Aeronautics	Aircraft, aero gas turbine engines and the interface of humans with aeronautic systems.	30	11
Electronics	Microelectronics, opto-electronics, electronic components, general-purpose equipment, fabrication equipment, and materials.	18	7
Marine Systems	Propulsors and propulsion systems, signature control for marine applications, subsurface and deep submergence vehicles.	19	6
Space Systems Technologies	Electronics, computers, optronics, propulsion, and sensors that power the US space industry.	14	5
Chemical and Biological Systems	Bioprocessing; chemical manufacturing; chemical and biologic defense systems; detection, warning, and identification equipment.	23	4
Guidance and Navigation and Vehicle Control	Technologies for flight management, guidance, and vehicle control that directly enhance the delivery accuracy and lethality of manned and unmanned guided and unguided weapons systems.	12	4
Manufacturing and Fabrication	Technologies required for the production of military hardware, including machine tools for advanced fabrication, production and processing. Also includes certain nondestructive evaluation and inspection equipment, bearings and certain robots.	14	4

[a] DSS percentages exceed 100 because one suspicious request sometimes targets two or more technologies.

IS related.[2] Defense contractors reported that 40 countries attempted to acquire sensitive technologies for IS during the year, more than any other single MCT.

The second most sought after category of militarily critical technology—based on the number of suspicious incidents reported by defense contractors in 2001—was **sensors and lasers**, with one-fifth of all elicitations. These technologies serve as the eyes and ears of many military systems, including those used to locate submarines, mines, and lost objects, but they also include technologies used commercially for locating fish and for seismic exploration at sea. A total of 38 foreign countries attempted to collect sensitive US information or technology relating to these products. Acoustic technology—much of it for passive sonar—accounted for almost 30 percent of the suspicious incidents and another third were for electro-optical sensors and lasers, technologies that are key to unmanned aerial vehicle (UAV) programs.

Armaments and energetic materials was the third most targeted technology group in 2001, accounting for 14 percent of total reported incidents. It attracted the attention of collectors in 27 countries, according to DSS data. The foreign interest is not surprising. This category includes the technologies used to develop and produce effective conventional munitions and weapons systems, such as ammunition; artillery; torpedoes; depth charges; high explosive, kinetic energy, and pyrotechnic warheads; propulsion systems; and fuzes, safing, and arming devices and their component parts.

Aeronautic technologies were also high on foreign collectors' shopping lists in 2001. In fact, 11 percent of the suspicious incidents reported by defense contractors in 2001 were aeronautic related. DSS data indicated that some 30 foreign countries targeted this technology. Recent international conflicts have repeatedly demonstrated the critical importance of air superiority for battlefield dominance, and many countries have attempted to upgrade their indigenous aviation programs by using proven US technologies.

[2] DSS calculates these figures by dividing the number of MCTs targeted by the number of suspicious targeting incidents. Since, in some targeting incidents, a collector attempts to acquire two or more MCTs, the percent figures inevitably sum to more than 100 percent.

Electronics technology filled out the top five MCTs that foreign collectors sought in 2001, accounting for 7 percent of all targeting. Defense contractors told DSS of being approached by representatives from 18 countries seeking electronics technology. Electronic technologies are either contained or used in the production of virtually every weapons system in the US arsenal. In addition, because much of this technology is dual-use, foreign companies and governments consider its acquisition important to ensuring development of a strong, efficient domestic industrial base.

Commercial Trade Secrets Still Attractive

Foreign collectors remained active in 2001 in the theft of commercial trade secrets. The Department of Justice's unclassified Web page made special note of eight prosecutions during 2001 under the Economic Espionage Act of 1996. Half of those cases involved foreign-born individuals, and all of the thefts were of trade secrets that had no military application. In two of the four cases, the technology went to foreign-owned firms, and in both of those cases the perpetrators were employees or ex-employees of the offended firms.

Technologies and proprietary information were not the only items sought by collectors. Confidential marketing information, such as that contained in contract bids and personal information on individuals who could be recruited to assist in the acquisition of proprietary information, were also considered high priority items last year.

Public- and Private-Sector Involvement

As in earlier years, the foreign sponsors of economic and industrial espionage in 2001 again came from both the public and private sectors. The DSS database shows that the collection effort was spread almost evenly among the various types of actors. Foreign government entities—including ministries, military attaches, government research and development centers, as well as state-owned companies, academies, and universities—were responsible for almost one-quarter of the suspicious activity in 2001. Another

20 percent of such incidents came at the hands of government-affiliated agencies or foreign companies that work solely or predominantly for foreign governments. Commercial businesses, with few ties to government, conducted 22 percent of suspicious activity, while individuals whom DSS could not identify as affiliated with any of the above categories accounted for another 14 percent. Finally, in some 20 percent of suspicious cases, it was impossible to identify whether the source was public or private or even whether the solicitation came from a group or individual. This unknown category included, for example, e-mail solicitations that contained no descriptors other than e-mail addresses and, hence, could fall into any of the categories.

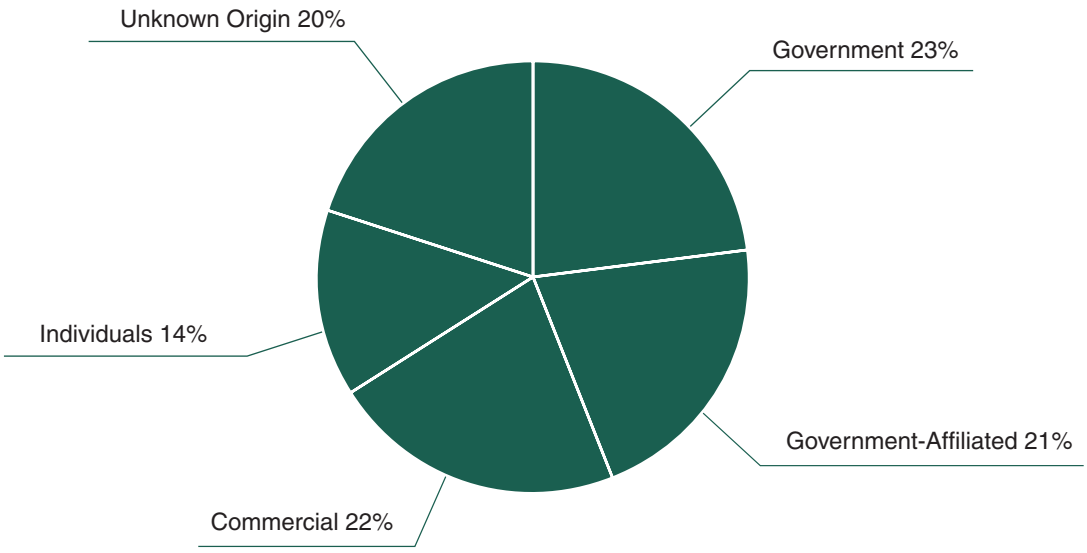
The Tools of Economic Collection and Industrial Espionage

Foreign collectors continued to employ a whole array of techniques against the United States in 2001, including legal and illegal methods, as well as human and electronic tools. The varied approaches have evolved to ensure full exploitation of potential weaknesses and vulnerabilities of the many accessible data sources.

Unsolicited Requests for Information

The simplest and most straightforward elicitation techniques were the ones most often employed in 2001. At the top of the list was the unsolicited request for information. Most such requests went to US Government organizations or to commercial enterprises that handle sensitive government projects. Requests ranged from legitimate inquiries for company publications and catalogues to efforts to elicit clearly restricted or sensitive data. Often the requests were for copies of technical papers, which corresponded to the technical expertise of the inquiring individual or company.

Figure 1: All Types of Collectors Were Actively Involved in 2001



Compiled from data provided by the Defense Security Service.

Most of the unsolicited requests—70 percent—came via e-mail, but letters and telephone calls were used as well. In general, those employing e-mail appear to have used the US company or university's Web site to obtain employee e-mail addresses prior to soliciting information. Often, e-mail is used to establish initial contact, cultivate common interests, and then collect. The anonymity of the Web allows collectors to solicit information with little or no tangible trail back to the host government or country.

Direct Attempts To Purchase

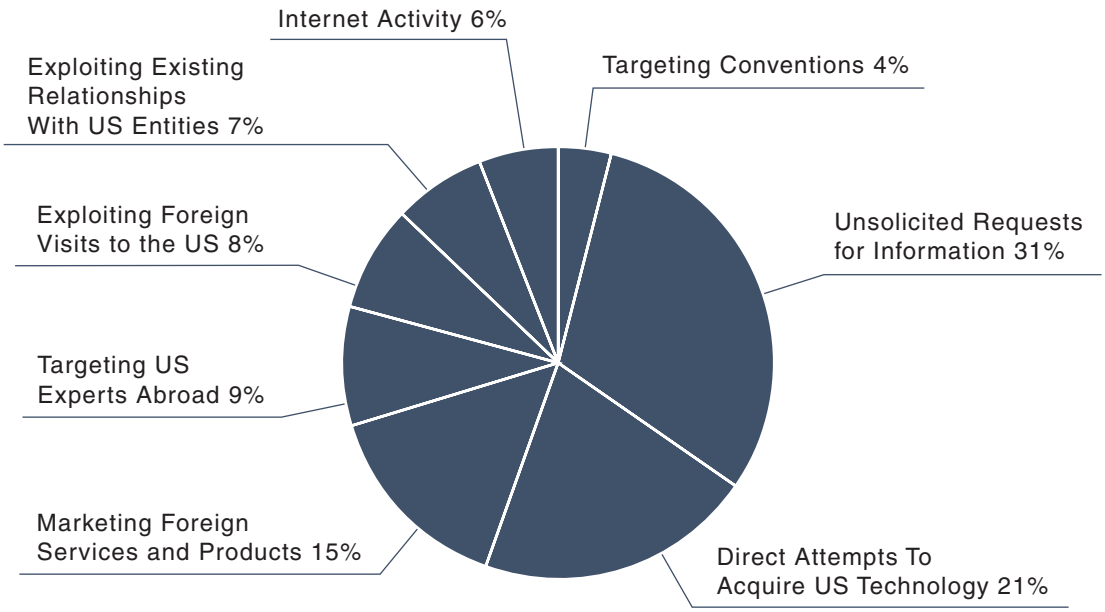
The second most popular technique for acquiring sensitive US goods in 2001 was the straightforward, direct attempt to purchase the technology. Foreign entities simply asked to purchase a particular item from US developers or dealers. Usually the items requested were export-controlled, and the requestors were frequently from embargoed countries. The success of such endeavors ultimately depended on the selling company's awareness of US laws, its security practices, and the honesty and integrity of management and employees.

Not all direct attempts to acquire US export-controlled equipment came from the true end users. Often, foreign front companies or intermediaries attempted the purchase on behalf of proscribed countries. The majority of these reported incidents involved dual-use products and technologies controlled under EAR or were military exportable items controlled under ITAR.

Marketing Foreign Services and Products

Another technique popular for gathering high-tech information in 2001 was the marketing of foreign services and products to US Government entities or to commercial firms that could be expected to have access to sensitive technology. In 15 percent of all suspicious incidents reported by cleared government contractors, foreign collectors attempted to insinuate themselves or their products into positions where they might gain access to high-tech goods. Companies, individuals, and research facilities were the heaviest users of this technique, but foreign governments were

Figure 2: Foreigners Use a Variety of Methods To Acquire US Technology



Compiled from data provided by the Defense Security Service.
Totals may not sum to 100 percent due to rounding error.

involved as well. Foreign commercial entities initiated 42 percent of the marketing attempts in 2001, followed by individuals at 20 percent, foreign government-affiliated interests at 12 percent, and government entities at 9 percent.

These marketing techniques took several forms. The most common technique was for foreign scientists and experts to apply to work in areas that would have given them access to sensitive US technologies. These requests were generally unsolicited and not in response to a vacancy notice. Foreign collectors with aeronautic and IS backgrounds, in particular, seemed to favor the marketing approach. Some of these incidents appear to be legitimate jobseekers looking for opportunities in the United States. But because of the high risks associated with giving supply chain access to foreign nationals, US contractors have been sensitive to such elicitations and have been quick to report any that seem suspicious.

The other common marketing technique used in 2001 was for foreign firms to offer hardware and software support. The rapidly expanding prowess of a number of countries in software and Web site development has given products from these countries widespread global appeal. Like employment offers, some of these probes were probably genuine attempts to market foreign software products and services for profit, but it is likely that a number of the overtures were ploys to gain access to DoD facilities and programs for the purpose of collecting information or mounting offensive cyber operations.

Exploiting US Experts Traveling Abroad

Foreign countries are becoming increasingly effective and aggressive in exploiting US experts traveling abroad, the fourth most utilized method for targeting US MCTs, according to DSS data. Short-term custodial detentions, including search and seizure by host-government officials at airports and waterways, accounted for 58 percent of the reported incidents in this category. These custodial detentions offered foreign officials the opportunity to gain information regarding US travelers' visits and to search the contents of laptop computers carried by the travelers.

Foreign intelligence services also continued to use electronic and human surveillance techniques to record conversations and track US visitors. Business executives and US Government officials alike reported being subjected to such tactics in 2001. US travelers were targeted for a broad range of MCTs in 2001. Information systems were targeted 36 percent of the time, aeronautics 19 percent, sensors and lasers 19 percent, space technology 5 percent, and armaments and energetic materials 5 percent.

Taking Advantage of Visits to the United States

Foreign companies and governments also continued to send visitors to the United States with the expressed intent of gathering economic and industrial intelligence. Such foreign visitors were involved in about 8 percent of the suspicious activities reported by government contractors in 2001. These guests—including one-time visitors as well as those in the United States on long-term visas—often had opportunities to observe sensitive US development and production processes up close. In fact, foreign visitors have long been regular fixtures at many sensitive sites, including military bases and research institutes. Once inside, some of the favorite techniques foreign visitors employed to gather information were wandering off from their group for unsupervised observations, lingering to engage a particular worker in conversation, and, when able, taking photographs.

The more than 500,000 foreign students currently studying in US colleges and universities are among the visitors who often have excellent access to sensitive technologies and who can funnel—legally and illegally—restricted or proprietary information to their native countries. A study of US universities in the mid-1990s revealed that roughly half of all Ph.D. students in computer science, engineering, math, and information science were foreign nationals, and most experts believe the ratio may be even higher today. Furthermore, about half of the foreign students studying in technical fields remain in the United States after receiving their degrees, often working for large, high-tech US companies.

A majority of student collection efforts in 2001 focused on open-source materials, such as university libraries, student laboratories, and unclassified databases. Historically, all thesis, term papers, and research studies completed by both students and faculty have been retained, databased, and made available to any individual with access to library facilities.

In addition to the authorized access students have to sensitive information, some have gained unauthorized access using "hacker" techniques and encryption software.

More than 80 percent of the visitors whom cleared US Government contractors reported as engaged in suspicious activity last year were either employees of, or directly affiliated with, foreign governments. Activities were judged as suspicious when visitors went beyond the bounds of their agreed upon visit protocols, to include wandering unescorted in restricted areas or asking for access to facilities or information outside the scope of approved activities.

More than one-third of the time that foreigner visitors were involved in suspicious activity in 2001, the technology targeted was IS. The other technologies that ranked high on the targeting lists of foreign visitors included armaments and energetic materials (23 percent) and aeronautics (15 percent).

Exploiting Relationships

One of the most effective tools that foreign collectors used to gain access to sensitive US information and technology in 2001 was exploiting new or existing relationships with US companies, organizations, or research institutes. Defense contractors reported that this method of attack was used in 7 percent of all suspicious targeting incidents in 2001. The preferred technique was the attempt to form joint ventures with US firms, but collectors also took advantage of relationships formed under foreign military sales provisions as well as training contracts.

These relationships place foreign collectors in direct contact with US technology providers in an environment of cooperation. Joint ventures can yield especially fruitful results because the foreign organization and the US provider become equity partners in the firm. Even the process of negotiating a joint venture—where no agreement is actually reached—can be a goldmine for foreign firms seeking to collect sensitive information. Training programs, which may include tours of sensitive facilities and previews of controlled technologies, give collectors serendipitous access to technologies that they might not otherwise see.

It is difficult to determine whether a foreign company pushing to form a relationship with a high-tech US firm is motivated primarily by the desire to transfer technology or by profits. There are, however, some common indicators when tech transfer is the driving force behind the agreement:

- Technology sharing proposals are clearly one sided in favor of the foreign partner.
- Partners submit repeated requests for unrestricted access to facilities or computer networks.
- Overstaffing by a foreign partner.
- Frequent questions that go beyond the scope of the relationship or that are directed to working-level personnel uncertain of rules regarding release of information.
- Specific inquiries about classified material.
- Repeated, focused requests to expand the boundaries of agreements to include denied technologies.

Given the considerable technology transfer benefits available through exploiting existing relationships, a number of countries have developed creative ways to facilitate the formation of these deals. Press reporting in 2001 indicated that some countries had established "incubators"—companies whose main function is to provide technical and financial assistance to foreign startup companies in the United States.

Perhaps because of the sizeable time and financial commitment that is often associated with establishing relationships, this tool was employed most frequently in 2001 by foreign government and government-affiliated organizations. More than 60 percent of the suspicious attempts to milk existing relationships with high-tech US entities came from foreign governments or from government-affiliated organizations. Only 19 percent of the suspicious efforts came from unaffiliated commercial enterprises, according to DSS reporting.

Foreign collectors tapped existing relationships to collect against the whole gamut of MCTs in 2001, but IS and armaments and energetic materials were the primary targets, according to defense contractors, each accounting for almost one-fourth of the suspicious

incidents. Sensors and lasers and aeronautics each attracted another 13 percent. The specific targets included military technologies related to Joint Direct Attack Munitions, Focal Plane Array systems, Arrow Missile air defense artillery program, multiple launch rocket systems, and Sparrow Missiles.

Closest "Friends," Greatest Risks

While any visit to a US high-tech firm offers foreign collectors a potentially lucrative environment, the richest collection environment is one in which foreign firms or governments have long-established relationships. In an area where foreigners are a common sight, it is easy for cleared US personnel to lower their guard and permit unauthorized access to controlled facilities. By becoming part of the fabric at a facility, foreign representatives may attempt to blur lines between classified and unclassified programs and gain access to restricted materials. Security personnel are more likely, under these circumstances, to attribute what may be a serious security breach by a foreign visitor to nothing more than an innocuous mistake by a "friend" or "partner" of the company.

Internet Activity

Internet-related targeting by foreign collectors slipped last year relative to the other collection methods. According to DSS reporting, the Internet was the seventh most actively used collection tool, down from sixth place in 2000. The composition of this category differs somewhat from that of the other collection techniques. DSS includes in this category not only incidents in which foreigners apparently attempted to use cyber tools to extract sensitive US information and technology—activities that are clearly under the rubric of economic collection and industrial espionage—but also foreign efforts to employ cyber weapons to damage US providers of those goods. Internet activity, as defined by DSS, includes hacking, probing, scanning, pinging, spamming, and virus infection. Suspicious e-mail inquiries to US firms were considered under the "direct request for information" category.

When defense contractors reported suspicious foreign Internet activity in 2001, 29 percent of the time they highlighted hacking incidents. Most hacking events

Defining Terms for the Cyber Threat

Hacker—*Once used as a slang term for a computer enthusiast, the term is now largely used to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data.*

Ping—*The use of cyber tools to check if a server is running. Pinging often precedes another form of cyber probe.*

Port scan—*A series of messages sent by someone attempting to break into a computer to learn which computer network services the computer provides. Port scanning gives a hacker an idea where to probe for weaknesses. Essentially, a port scan consists of sending a message to each port, one at a time. The kind of response received indicates whether the port is used and can, therefore, be probed for weakness.*

Probe—*Searches initiated at remote sites with the intent of determining potential weaknesses in systems for exploitation.*

Spam—*An inappropriate attempt to use a mailing list as if it was a broadcast medium by sending the same message to a large number of people who have not requested it. The practice can disrupt business by tying up computers and personnel resources.*

Virus—*A program or piece of code that is loaded onto a computer without the owner's knowledge and that runs against the owner's wishes. Viruses can also replicate themselves. Even a simple virus can be dangerous because it could quickly use all available memory and bring the system to a halt. An even more dangerous type of virus is one capable of transmitting itself across networks and bypassing security systems. Some people distinguish between general viruses and worms. A worm is a special type of virus that can replicate itself and use memory but cannot attach itself to other programs.*

ended in site defacements, but they also included attempts to penetrate firewalls apparently for the purpose of downloading sensitive information or inserting trapdoors for later downloading. Spam accounted for about 20 percent of suspicious Internet activity, followed by computer probes (17 percent), virus attacks (10 percent), and port scans (7 percent).

Most US cleared facilities advertise in some form on the Web, making them attractive targets for solicitation or attack. One key advantage of using the Web is that mail servers provide the technical means to make collectors or attackers virtually anonymous, enabling them to seek information without necessarily identifying themselves or their country of origin. The Internet has also been used as a tool for spotting and assessing individuals who may be willing and able to provide insider information. In a practice known as "cyberspotting," an intelligence service identifies potential recruits by using the Internet to canvass résumés and to track responses to surveys.

There are at least two competing possible explanations for the apparent relative decline in use of the Internet in 2001 as a means to access US technology. First, US vendors, aware of the potential technological losses through cyber penetration, may have become more effective at protecting sensitive information either through encryption or by simply removing data from public Web sites. In the face of reduced prospects for success, targeting countries may have relied more heavily on other—more viable—collection techniques. Alternatively, foreign collectors seeking US technology may have become more sophisticated at masking their efforts. In that case, a decline in reporting may reflect not a downward trend in Internet activity but, rather, a reduction in the number of detected efforts. A DoD study conducted in the mid-1990s determined that more than 60 percent of all computer attacks went undetected. While detection techniques have improved since the survey was conducted, so too have attack methods, and it is unlikely that the detection rate has risen significantly.

International Conventions, Symposiums, and Business Meetings

The numerous scientific and business meetings held in the United States also continued to serve as useful venues for foreign collectors to gather information on sensitive US technologies, although this technique was used in only 4 percent of the reported suspicious incidents in 2001. Foreign scientists and technical experts who attended such meetings often worked directly on sensitive projects in their home countries and, hence, were perfectly situated to gather information to fill critical gaps. The collegial atmosphere at these meetings fosters a give-and-take process conducive to gathering controlled information. Even when kept at an unclassified level, discussions on the sidelines of these meetings can become so technical as to pass along valuable information that would not be releasable to foreign nationals due to export controls.

The invitation process also can yield valuable technology gains for collectors. Conference sponsors often request that attendees send technical papers or brief aspects of their research to demonstrate expertise. In attempting to demonstrate proficiency, experts may inadvertently release sensitive—and sometimes even protected—data. Conferences may also be useful tools for gleaning valuable targeting information on US facilities and expertise. Registration forms usually require biographic details about individuals—including corporate experience and areas of expertise—that can be useful in assessing an individual or firm's access to sensitive programs. In addition, personal name cards collected at conferences are commonly used in the targeting process.

The Attacking Countries

The laundry list of countries seeking US technologies in 2001 was long and diverse. Some 75 countries were involved in one or more suspicious incidents.

The most active countries in economic espionage, according to DSS data, were an interesting mix of rich and poor and "friend" and foe. Many of the richest nations aggressively sought the latest in advanced technologies both to upgrade their already formidable military infrastructures—particularly command, control, and communications—and to make their already

sophisticated industries even more competitive with the United States. Most of the poorer countries, however, continued to exhibit a preference for older "off the shelf" hardware and software to renovate their existing defensive systems and to develop countermeasures to provide them battlefield advantage. The search for lower technology goods by these less developed countries probably reflected their desire to bring in technologies that could be more easily integrated into their existing military structures; a number of these countries were probably not capable of utilizing the most sophisticated US technologies. Many of these acquisitions are no longer classified and often have both military and civilian applications. These included so-called dual-use technologies controlled for export under the EAR and items controlled under the ITAR.

The Road Ahead

There is every indication that, as aggressive and clever as past efforts to access sensitive US technology have been, those efforts will become only more intense and more sophisticated over the next few years. The massive US research and development program ensures that state-of-the-art technology will continue to originate in the United States, and the openness of US society will make that technology readily accessible to foreign countries—friend and foe alike.

Foreign countries will continue to employ the whole gamut of collection tools over the next few years. All of the major players recognize that maximum flexibility is the key to success. When one method fails, collectors will inevitably take a different approach. Naturally, the easiest methods—requests for information; direct acquisition; and solicitation and marketing—will continue to be the first employed, but none of the other tools will be discarded. Virtually all major collectors seem poised to take greater advantage of the Internet in the future as both a collection and disruption tool, though the extent of activity will continue to be difficult to gauge. Given the Internet's expanding global reach, all forms of Internet activity—using Web sites to locate technology, e-mail to solicit technology, and cyber attacks to unwittingly extract technology—will probably jump sharply over the next few years.

Although we have no evidence to date that foreign countries have attempted to insert malicious code into products sold to the United States, remote and supply-chain attacks are major threats for the future. Foreign firms are becoming dominant in the production of key IT hardware components and software, and it is possible in the future that such products could even end up in highly classified closed systems. In that event, there would be opportunities to introduce difficult-to-detect code capable of corrupting those systems or, perhaps more importantly, of covertly sending sensitive information back to foreign providers.

As to the types of MCTs that will be of interest over the next few years, we believe IS will continue to top the collectors' lists. The central role that it will play in economic and military development would, by itself, be enough to ensure IS the top spot. Add to that the need to acquire the most recent hardware and software technology to either stave off cyber attacks or to develop offensive cyber capabilities, and you have an even more potent lure for foreign collectors.

Other MCTs that will attract increased attention include the following:

- Aeronautics; guidance, navigation, and vehicle control systems; and sensors and lasers are certain to remain hot items. The recent success of US airpower, UAVs, and smart-weapons in South Asia means that countries possessing even a modest capability to produce airframes will aggressively pursue this technology. Countries that buy aircraft off the shelf will seek these technologies to upgrade.

- Space systems technology, which in 2001 attracted a relatively small share of foreign collection interest, may rate higher priorities in the future. In particular, any successes in US efforts to develop a missile defense system would be closely monitored and would probably spur a flurry of new interest in acquiring space-based technologies.